Joseph Silva Jr.

SNHU

CS 405: 5-1 Case Study

11/27/2021

## Contents

[Introduction 3](#_Toc52464053)

[Describe](#_Toc52464054) Breach 3

[Identify the threat(s) 4](#_Toc52464055)

[Prevent Breaches 4](#_Toc52464056)

[Triple A and Defense in Depth 4](#_Toc52464057)

[Reference 6](#_Toc52464058)

**Introduction**

* Name of case and link – Blueleaks & <https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/>
* Date of case – June 20, 2020
* Why did this case make the news? – The case made the news because the data that was leaked affected many law enforcement agencies throughout the US by making an officer’s personal information public knowledge and making confidential or classified information public knowledge. It was the largest computer hacking of law enforcement agencies and data by a group known as “DDoSecrets”.

**Describe the breach**

* Type of security or data breach or combination – The security breach almost 270 gigabytes of thousands of sensitive files from law enforcement agencies and the private sectors stored at fusion centers. These files contained information on members of law enforcement, information on terrorism, evidence, informants’ information, confidential information on ongoing and closed cases, etc.
* Why was this company a target? – The fusion centers were targeted because they were state owned entities that collected information and provided access to this information to law enforcement agencies in order to assist these LE agencies to stay in communication with each other and to allow the LEOs to have current information of subjects and events by the help of other agencies. These centers were under attack by hackers because law enforcement was under scrutiny due to events such as the murder of George Floyd by law enforcement officers and hackers were attempting to put out information to show any wrong doings by LEOs.

**Identify the threat(s)**

* Immediate threat(s) – The immediate threats would be putting individuals’ lives in jeopardy. Individuals such as a law enforcement officers, undercover officers, DAs, judges, juries, and confidential informants’ information placed as public record, and this gave criminals the ability to search for these individuals to commit other crimes such as witness intimidation and/or assaults.
* Potential threat(s) if the vulnerability goes unresolved – The potential threats would be a continuous situation in placing these individuals in danger when it came to making arrests and obtaining evidence on crimes from dangerous individuals. The continuation of this vulnerability would have caused issues within the criminal justice system when it came to the safety of personnel and evidence.

**What could a developer have done to prevent this breach?**

* Which policy or policies will help prevent this type of attack? – Breaching or attempt breaching alerts, routine tests with log in, routine user checkups, login lockouts, and third-party database audits.

**Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.**

* Authentication – With these third-party information sites, individuals must send in registration information and the information also must have contact information for a supervisor in order the third party to verify the individual being a member of law enforcement or a security private sector. After the registration process, the contact information for the individual must not be a private email account such as Gmail or yahoo email accounts. The emails must be business or government accounts in order to gain access to the database. Lastly, the database has its own username and password log in for the individual to enter the database.
* Authorization – An authorization that is sometimes used with these third-party law enforcement information databases is only allowing government or corporate network must be required to allow access to the url for the fusion center’s database. These prevents hackers from invading a device attached to a public network or a civilian network which may not always have the safety precautions of a government or corporate network firewalls.
* Accounting – The third-party databases and also the user’s networks document when certain data was accessed and who accessed the database, which usually can be found during an audit.
* Defense in depth – The databases have the multiple authentications from registration to log in access. The databases also can be audited on any occasion to verify when a user accessed information in the fusion center. The network also uses multiple firewalls to protect any malware or intrusion into the database. Lastly, the updated defense after events such as blue leaks would be only being able to access the URL on a government or corporation network.

**Reference:**

1. 22, T. S. S. J., 22, D. S. J., 22, T. F. J., 22, P. C. J., 22, Z. J., 22, Z. J., 22, pic J., 22, Z. D. J., 23, M. J., 23, D. R. J., 23, A. J., 23, needmorename J., 30, S. B. J., 23, security vet J., 23, S. J., 25, S. J., 23, B. B. J., 22, R. F. O. L. J., 22, Q. E. O. G. J., … 14, globaltel J. (2020, June 22). *'blueleaks' exposes files from hundreds of police departments*. Krebs on Security. Retrieved November 27, 2021, from https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/.